MODELLO DI ORGANIZZAZIONE GESTIONE E CONTROLLO

Al SENSI

DEL DECRETO LEGISLATIVO 8 GIUGNO 2001, n. 231

PARTE SPECIALE C

ART. 24 BIS DEL D.LGS.231/01

I REATI DI CUI ALL'ART. 24-8IS DEL DECRETO LEGISLATIVO 231/01: ESEMPI DELLE PRINCIPALI POSSIBILI MODALITA DI COMMISSIONE

Nel presente capitolo è illustrato ii contenuto dei cosiddetti "Reati Informatici" previsti dall'art. 24-bis del D. Lgs. 231/2001, e ritenuti astrattamente ipotizzabili per Brain-it (d'ora innanzi, per brevità, "la Società") - nonché un'esposizione delle principali possibili modalità di attuazione dei suddetti reati - al fine di consentire l'acquisizione di nozioni utili alla comprensione del Modello e della presente Parte Speciale.

Documenti informatici **art. *491 bis* c.p.**

"Se alcuna delle falsità previste dal presente capo riguarda un documento informatico pubblico o privato, avente efficacia probatoria, si applicano le disposizioni del Capo stesso concernenti rispettivamente gli atti pubblici e le scritture private. "

La norma sopra citata conferisce valenza penale alla commissione di reati di falso attraverso l'utilizzo di documenti informatici; i reati di falso richiamati sono i seguenti:

- Falsità materiale commessa dal pubblico ufficiale in atti pubblici (art. 476 c.p.):

"II pubblico ufficiale, che, nell'esercizio de/le sue funzioni, forma, in tutto o in parte, un atto falso o altera un atto vero, è punito con la reclusione da uno a sei anni. Se la falsità concerne un atto o parte di un atto, che faccia fede fino a querela di falso, la reclusione è da tre a dieci anni".

- Falsità materiale commessa dal pubblico ufficiale in certificati o autorizzazioni amministrative (art. 477 c.p.):

"II pubblico ufficiale, che, nell'esercizio delle sue funzioni, contraffà o altera certificati o autorizzazioni amministrative, ovvero, mediante contraffazione o alterazione, fa apparire adempiute le condizioni richieste per la loro validità, è punito con la reclusione da sei mesi a tre anni".

- Falsità materiale commessa dal pubblico ufficiale in copie autentiche di atti pubblici o privati e in attestati del contenuto di atti (art. 478 c.p.):

"II pubblico ufficiale, che, nell'esercizio delle sue funzioni, supponendo esistente un atto pubblico o privato, ne simula una copia e la rilascia in forma legale, ovvero rilascia una copia di un atto pubblico o privato diversa dall'originale, è punito con la reclusione da uno a quattro anni. Se la falsità concerne un atto o parte di un atto, che faccia fede fino a querela di falso, la reclusione è da tre a otto anni. Se la falsità è commessa dal pubblico ufficiale in un attestato sul contenuto di atti, pubblici o privati, la pena e della reclusione da uno a tre anni':

- Falsità ideologica commessa dal pubblico ufficiale in atti pubblici (art. 479c.p.):

"II pubblico ufficiale, che, ricevendo o formando un atto nell'esercizio delle sue funzioni, attesta falsamente che un fatto è stato da Lui compiuto o è avvenuto alla sua presenza, o attesta come da Lui ricevute dichiarazioni a Lui non rese, ovvero omette o altera dichiarazioni da lui ricevute, o comunque attesta falsamente fatti dei quali l'atto è destinato a provare la verità, soggiace alle pene stabilite nell'articolo 476

- Falsità ideologica commessa dal pubblico ufficiale in certificati o autorizzazioni amministrative (art. 480 c.p.):

"II pubblico ufficiale, che, nell'esercizio delle sue funzioni, attesta falsamente, in certificati o autorizzazioni amministrative, fatti dei quali l'atto è destinato a provare la verità, è punito con la reclusione da tre mesi a due anni".

- Falsità ideologica in certificati commessa da persone esercenti un servizio di pubblica necessita (art. 481 c.p.):

"Chiunque, nell'esercizio di una professione sanitaria o forense, o di un altro servizio di pubblica necessita, attesta falsamente, in un certificato, fatti dei quali l'atto è destinato a provare la verità, è punito con la reclusione fino a un anno o con la multa da € 51,00 a € 516,00. Tali pene si applicano congiuntamente se il fatto è commesso a scopo di lucro:

- Falsità materiale commessa dal private (art. 482 c.p.):

"Se alcuno dei fatti preveduti dagli articoli 476, 477 e 478 è commesso da un privato, ovvero da un pubblico ufficiale fuori dell'esercizio de/le sue funzioni, si applicano rispettivamente le pene stabilite nei detti articoli, ridotte di un terzo':

- Falsità ideologica commessa dal privato in atto pubblico (art. 483 c.p.):

"Chiunque attesta falsamente al pubblico ufficiale, in un atto pubblico, fatti dei quali l'atto è destinato a provare la verità, è punito con la reclusione fino a due anni. Se si tratta di false attestazioni in atti dello stato civile, la reclusione non può essere inferiore a tre mesi

- Falsità in registri e notificazioni (art. 484c.p.):

"Chiunque, essendo per Legge obbligato a fare registrazioni soggette all'ispezione dell'Autorità di pubblica sicurezza, o a fare notificazioni all'Autorità stessa circa le proprie operazioni industriali, commerciali o professionali, scrive o faccia scrivere false indicazioni è punito con la reclusione fino a sei mesi o con la multa fino a €309,00':

- Falsità in scrittura privata (art. 485 c.p.):

"Chiunque, al fine di procurare a se o ad altri un vantaggio o di recare ad altri un danno, forma, in tutto o in parte, una scrittura privata falsa, o altera una scrittura privata vera, e punito, qualora ne faccia uso o lasci che altri ne faccia uso, con la reclusione da sei mesi a tre anni. Si considerano alterazioni anche le aggiunte falsamente apposte a una scrittura vera, dopo che questa fu

definitivamente formata".

- Falsità
- in foglio firmato in bianco. Atto privato (art. 486 c.p.):

"Chiunque, al fine di procurare a se o ad altri un vantaggio o di recare ad altri un danno, abusando di un foglio firmato in bianco, de/ quale abbia ii possesso per un titolo che importi l'obbligo o la facoltà di riempirlo, vi scrive o fa scrivere un atto privato produttivo di effetti giuridici, diverso da quello a cui era obbligato o autorizzato, è punito, se del foglio faccia uso o lasci che altri ne facciano uso, con la reclusione da sei mesi a tre anni. Si considera firmato in bianco ii foglio in cui ii sottoscrittore abbia lasciato bianco un qualsiasi spazio destinato a essere riempito".

- Falsità in foglio firmato in bianco. Atto pubblico (art. 487 c.p.):

"II pubblico ufficiale, che, abusando di un foglio firmato in bianco, del quale abbia ii possesso per ragione del suo ufficio e per un titolo che importa l'obbligo o la facoltà di riempirlo, vi scrive o vi fa scrivere un atto pubblico diverso da quello a cui era obbligato o autorizzato, soggiace alle pene rispettivamente stabilite negli articoli 479 e 480".

- Altre falsità in foglio firmato in bianco. Applicabilità delle disposizioni sulle falsità materiali (art. 488 c.p.):

"Ai casi di falsità su un foglio firmato in bianco diversi da quelli preveduti dai due articoli precedenti, si applicano le disposizioni sulle falsità materiali in atti pubblici o in scritture private".

- Uso di atto falso (art. 489 c.p.):

"Chiunque, senza essere concorso nella falsità, fa uso di un atto falso soggiace alle pene stabilite negli articoli precedenti, ridotte di un terzo. Qualora si tratti di scritture private, chi commette il fatto è punibile soltanto se ha agito al fine di procurare a se o ad altri un vantaggio o di recare ad altri un danno".

- Soppressione, distruzione e occultamento di atti veri (art. 490c.p.):

"Chiunque, in tutto o in parte, distrugge, sopprime od occulta un atto pubblico o una scrittura privata veri soggiace rispettivamente a/le pene stabilite negli articoli 476, 477, 482 e 485, secondo le distinzioni in essi contenute. Si applica la disposizione del capoverso dell'articolo precedente':

- Copie autentiche che tengono luogo degli originali mancanti (art. 492c.p.):

"Agli effetti delle disposizioni precedenti, nella denominazione di "atti pubblici" e di "scritture private" sono compresi gli atti originali e le copie autentiche di essi, quando a norma di legge tengano in luogo degli originali mancanti':

Falsità commesse da pubblici impiegati incaricati di un servizio pubblico (art. 493 c.p.):
"Le disposizioni degli articoli precedenti sulle falsità commesse da pubblici ufficiali si applicano altresì agli impiegati dello Stato, o di un altro ente pubblico, incaricati di un pubblico servizio relativamente agli atti che essi redigono nell'esercizio delle loro attribuzioni".

La norma stabilisce che tutti i delitti relativi alla falsità in atti disciplinati dal Codice Penale (cfr. Capo 111, Titolo VII, Libra 11), tra i quali rientrano sia le falsità ideologiche che le falsità materiali, sia in atti pubblici che in atti privati, sono punibili anche nel caso in cui la condotta riguardi non un documento cartaceo bensì un documento informatico, pubblico o privato, avente efficacia probatoria (in quanta rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti). In particolare, si precisa che si ha "falsità materiale" quando un documento viene formato o sottoscritto da persona diversa da quella indicata come mittente sottoscrittore, con divergenza tra autore apparente e autore reale del documento (contraffazione} ovvero quando ii documento è artefatto (e, quindi, alterato} per mezzo di aggiunte o cancellazioni successive alla sua formazione. Si ha, invece, "falsità ideologica" quando un documento non è veritiero nel senso che, pur non essendo ne contraffatto ne alterato, contiene dichiarazioni non vere. Nel falso ideologico, dunque, e lo stesso autore del documento che attesta fatti non rispondenti al vero. I documenti informatici, pertanto, sono equiparati a tutti gli effetti ai documenti tradizionali.

A titolo esemplificativo, integra ii delitto di falsità in documenti informatici la condotta di chi:

falsifichi documenti aziendali oggetto di flussi informatizzati;

alteri informazioni a valenza probatoria presenti sui propri sistemi allo scopo di eliminare dati considerati "sensibili" in vista di una possibile attività ispettiva.

Accesso abusivo ad un sistema informatico o telematico (art. 615-terc.p)

"Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contra la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni. La pena è della reclusione da uno a cinque anni:

se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema;

se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato;

se dal fatto deriva la distruzione o ii danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti.

Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni.

Nel caso previsto dal primo comma ii delitto è punibile a querela della persona offesa; negli altri casi si procede d'ufficio. "

Tale reato si realizza quando un soggetto si introduca abusivamente in un sistema informatico o telematico protetto da misure di sicurezza.

A tal riguardo si sottolinea come il legislatore abbia inteso punire l'accesso abusivo ad un sistema informatico o telematico tout court, e dunque anche quando, ad esempio, all'accesso non segua un vero e proprio danneggiamento di dati: si pensi all'ipotesi in cui un soggetto acceda abusivamente ad un sistema informatico e proceda alla stampa di un documento contenuto nell'archivio del personal computer altrui, pur non effettuando alcuna sottrazione materiale di file, ma limitandosi ad eseguire una copia (accesso abusivo in copiatura), oppure procedendo solo alla visualizzazione di informazioni (accesso abusivo in sola lettura).

La suddetta fattispecie delittuosa si realizza altresì nell'ipotesi in cui ii soggetto agente, pur essendo entrato legittimamente in un sistema, vi si sia trattenuto contra la volontà del titolare del sistema, nonché, secondo il prevalente orientamento giurisprudenziale, qualora il medesimo abbia utilizzato il sistema per ii perseguimento di finalità differenti da quelle per le quali era stato autorizzato.

II delitto potrebbe pertanto essere astrattamente configurabile nell'ipotesi in cui un soggetto acceda abusivamente ai sistemi informatici di proprietà di terzi (outsider hacking), per prendere cognizione di dati riservati altrui nell'ambito di una negoziazione commerciale, a acceda abusivamente ai sistemi aziendali della società per acquisire informazioni alle quali non avrebbe legittimo accesso in vista del compimento di atti ulteriori nell'interesse della società stessa.

La disposizione contenuta nell'ultimo comma appresta una tutela più intensa, attraverso l'inasprimento della pena, a taluni sistemi informatici, che, per la funzione svolta e per ii rilevante interesse pubblico, si appalesano come beni di primaria importanza.

Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o te[ematici (art. 15-quater c.p.I)

"Chiunque, al fine di procurare a se o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei a/l'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, e punito con la reclusione sino ad un anno e con la multa sino a euro 5.164.

La pena è della reclusione da uno a due anni e della multa da euro 5.164 a euro 10.329 se ricorre taluna de/le circostanze di cui ai numeri 1) e 2) del quarto comma dell'articolo 617-quater."

Tale reato si realizza qualora un soggetto, al fine di procurare a se o ad altri un profitto a di arrecare ad altri un danno, abusivamente si procuri, riproduca, diffonda, comunichi a consegni codici, parole chiave a altri mezzi idonei all'accesso a un sistema informatico o telematico protetto da misure di sicurezza, o comunque fornisca indicazioni o istruzioni idonee a raggiungere tale scopo.

L'art. 615-quater c.p., pertanto, punisce le condotte preliminari all'accesso abusive poiché consistenti nel procurare a se o ad altri la disponibilità di mezzi di accesso necessari per superare le barriere protettive di un sistema informatico.

I dispositivi che consentono l'accesso abusive ad un sistema informatico sono costituiti, ad esempio, da codici, password o schede informatiche (quali badge o smart card). Tale fattispecie si configura sia nel caso in cui ii soggetto, in possesso legittimamente dei dispositivi di cui sopra (ad esempio, un operatore di sistema), Ii comunichi senza autorizzazione a terzi soggetti, sia net caso in cui tale soggetto si procuri illecitamente uno di tali dispositivi.

L'art. 615-quater c.p., inoltre, punisce chi rilascia istruzioni o indicazioni che rendano possibile la ricostruzione del codice di accesso oppure ii superamento delle misure di sicurezza.

Potrebbe rispondere del delitto, ad esempio, ii dipendente della società (A) che comunichi a un altro soggetto (8) la password di accesso alle caselle e-mail di un proprio collega (C), allo scopo di garantire a B la possibilità di controllare le attività svolte da C, quando da ciò possa derivare un determinate vantaggio o interesse per la società.

***Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (.art. 615- quinquies* c.p.)**

"Chiunque, a/lo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, si
procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altre apparecchiature, dispositivi o programmi informatici, è punito con la reclusione fino a due anni e con la multa sino a euro 10.329".

Tale reato si realizza qualora qualcuno, alto scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti, o ad esso pertinenti, ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, si procuri, produca, riproduca, importi, diffonda, comunichi, consegni o, comunque, metta a disposizione di altre apparecchiature, dispositivi o programmi informatici.

Tale delitto potrebbe, ad esempio, configurarsi qualora un dipendente si procuri un Virus idoneo a danneggiare o a interrompere ii funzionamento del sistema informatico aziendale in modo da distruggere documenti "sensibili" in relazione ad un procedimento penale a carico della società.

Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-quaterc.p.)

"Chiunque fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe, è punito con la reclusione da sei mesi a quattro anni.

Salvo che ii fatto costituisca più grave reato, la stessa pena si applica a chiunque rive/a, mediante qua/siasi mezzo di informazione al pubblico, in tutto o in parte, ii contenuto de/le comunicazioni di cui al primo comma. I delitti di cui ai commi primo e secondo sono punibili a querela de/la persona offesa.

Tuttavia, si procede d'ufficio e la pena è della reclusione da uno a cinque anni se il fatto è commesso:

in danno di un sistema informatico o telematico utilizzato dal/o Stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessita;

da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti al/a funzione o al servizio, ovvero con abuso della qualità di operatore de/ sistema;

da chi esercita anche abusivamente la professione di investigatore privato."

Tale ipotesi di reato si configura qualora un soggetto fraudolentemente intercetti comunicazioni relative a un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero impedisca o interrompa tali comunicazioni, nonché nei casi in cui un soggetto riveli, parzialmente o integralmente, ii contenuto delle comunicazioni al pubblico mediante qualsiasi mezzo di informazione.

Attraverso tecniche di intercettazione e possibile, durante la fase della trasmissione di dati, prendere cognizione del contenuto di comunicazioni tra sistemi informatici o modificarne la destinazione: l'obiettivo dell'azione e tipicamente quello di violare la

riservatezza dei messaggi, ovvero comprometterne l'integrità, ritardarne o impedirne l'arrivo a destinazione. II reato potrebbe configurarsi, ad esempio, con ii vantaggio concreto della società, nel caso in cui un dipendente impedisca una determinata comunicazione in via informatica al fine di evitare che un'impresa concorrente trasmetta i dati e/o l'offerta per la partecipazione a una gara.

II reato in questione e un reato comune, realizzabile ad opera di chiunque. 114° comma, tuttavia, prevede una serie di circostanze aggravanti, in presenza delle quali ii delitto, perseguibile a querela delle persone offese nelle ipotesi contemplate dai primi due commi, diviene perseguibile d'ufficio con contestuale aumento delta pena. Tali aggravanti riguardano la qualità soggettiva dell'agente (pubblico ufficiale, incaricato di un pubblico servizio, investigatore privato e operatore del sistema) o la qualità oggettiva del sistema informatico o telematico in danno del quale si agisce (".... utilizzato dallo Stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessita").

Installazione di apparecchiature atte ad impedire, intercettare o interrompere comunicazioni informatiche o telematiche (art. 617-quinquies c.p.>

"Chiunque, fuori dai casi consentiti dalla legge, installa apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi, e punito con la reclusione da uno a quattro anni. La pena è della reclusione da uno a cinque anni nei casi previsti dal quarto comma dell'articolo 617- quater."
Questa fattispecie di reato si realizza quando qualcuno, fuori dai casi consentiti dalla legge, installi apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi.

La condotta vietata dall'art. 617-quinquies c.p. è, pertanto, costituita dalla mera installazione delle apparecchiature, a prescindere dalla circostanza che le stesse siano o meno utilizzate, purché le stesse

abbiano una potenzialità lesiva.

II reato si integra, ad esempio, a vantaggio della società, nel caso in cui un dipendente si introduca fraudolentemente presso la sede di una potenziale controparte commerciale al fine di installare apparecchiature idonee all'intercettazione di comunicazioni informatiche o telematiche rilevanti in relazione ad una futura negoziazione.

Danneggiamento di informazioni dati e programmi informatici tart. 635-bis c.p.≥ "Salvo che ii fatto costituisca più grave reato, chiunque distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui è punito, a querela

della persona offesa, con la reclusione da sei mesi a tre anni. Se ricorre la circostanza di cui al numero 1) del secondo comma del/'artico/o 635 ovvero se ii fatto è commesso con abuso de/la qua/ita di operatore del sistema, la pena è de/la reclusione da uno a

quattro anni e si procede d'ufficio"

Tale fattispecie di reato si realizza quando un soggetto distrugga, deteriori, cancelli, alteri o sopprima informazioni, dati o programmi informatici altrui. II danneggiamento potrebbe essere commesso a vantaggio della società laddove, ad esempio, l'eliminazione o l'alterazione dei file o di un programma informatico appena acquistato siano poste in essere al fine di far venire meno la prova del credito da parte di un fornitore della società o al fine di contestare ii corretto adempimento delle obbligazioni da parte del medesimo o, ancora, nell'ipotesi in cui vengano danneggiati dei dati aziendali "compromettenti".

Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo stato o da altro Ente Pubblico o comunale di pubblica utilità: art. 35-terc.

*"*Salvo che il fatto costituisca più grave reato, chiunque commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità, è punito con la reclusione da uno a quattro anni. Se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, dei dati o dei programmi informatici, la pena e de/la reclusione da tre a otto anni.

Se ricorre la circostanza di cui al numero 1) del secondo comma dell'artico/o 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata."

Tale reato si realizza quando un soggetto commetta un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità.

Tale delitto si distingue dal precedente poiché, in questo caso, ii danneggiamento ha ad oggetto beni dello Stato o di altro ente pubblico o, comunque, di pubblica utilità; ne deriva che ii delitto sussiste anche nel caso in cui si tratti di dati, informazioni o programmi di proprietà di privati ma destinati al

soddisfacimento di un interesse di natura pubblica.

Tale reato potrebbe ad esempio essere commesso nell'interesse della società, qualora un dipendente compia atti diretti a distruggere documenti informatici aventi efficacia probatoria, registrati presso enti pubblici (es. polizia giudiziaria), relativi a un procedimento penale a carico della società.

Danneggiamento di sistemi informatici o telematici (art. 635-quaterc.p.)

"Salvo che ii fatto costituisca più grave reato, chiunque, mediante le condotte di cui all'artico/o 635-bis, ovvero attraverso l'introduzione o *la trasmissione di dati, informazioni* o *programmi, distrugge, danneggia, rende, in tutto* o *in parte, inservibili sistemi informatici* o *telematici altrui* o *ne ostacola gravemente ii funzionamento è punito con la reclusione da uno* a *cinque anni. Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero* se *ii fatto è* commesso *con abuso della qualità di operatore del sistema, la pena è aumentata."*

Questo reato si realizza quando un soggetto mediante le condotte di cui all'art. 635-bis c. p., ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugga, danneggi, renda, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacoli gravemente ii funzionamento. Pertanto qualora l'alterazione dei dati, delle informazioni o dei programmi renda inservibile o ostacoli gravemente ii funzionamento del sistema si integrerà ii delitto di danneggiamento di sistemi informatici e non quello di danneggiamento dei dati previsto dall'art. 635-bis c.p.

Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 35: quinguies c.p)

"Se il fatto di cui all'artico/o 635-quater è diretto a *distruggere, danneggiare, rendere, in tutto* o *in parte, inservibili sistemi informatici* o *telematici di pubblica utilità* o *ad ostacolarne gravemente ii funzionamento, la pena è della reclusione da uno* a *quattro anni. Se dal fatto deriva la distruzione* o *ii danneggiamento del sistema informatico* o *telematico di pubblica utilità ovvero se questo è reso, in tutto* o *in parte, inservibile, la pena*

è della reclusione da tre a *otto anni. Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata".*

Questo reato si configura quando la condotta di cui al precedente art. 635-quater c.p. è diretta a distruggere, danneggiare, rendere in tutto o in parte inservibili, sistemi informatici o telematici di pubblica utilità o a ostacolarne gravemente ii funzionamento. Nel delitto di danneggiamento di sistemi informatici o telematici di pubblica utilità, differentemente dal delitto di danneggiamento di dati, informazioni e programmi di pubblica utilità di cui all'art. 635-ter c.p, quel che rileva è in primo luogo che ii danneggiamento deve avere ad oggetto un intero sistema e, in secondo luogo, che ii sistema sia utilizzato per ii perseguimento di pubblica utilità, indipendentemente dalla proprietà privata o pubblica dello stesso.

Frode Informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 64O-quinguies c.p.>

"II soggetto che presta servizi di certificazione di firma elettronica, il quale, al fine di procurare a *se* o *ad altri un ingiusto profitto ovvero di arrecare ad altri danno, viola gli obblighi previsti dalla legge per il rilascio di un certificato qualificato, è punito con la reclusione fino* a *tre anni e con la multa da 51* a *1.032 euro"*

Questo reato si configura quando un soggetto che presta servizi di certificazione di Firma Elettronica, al fine di procurare a sé o ad altri un ingiusto profitto, ovvero di arrecare ad altri danno, violi gli obblighi previsti dalla legge per il rilascio di un certificato qualificato.

Tale reato è dunque un reato e proprio in quanto tale può essere commesso solo da parte dei certificatori qualificati, o meglio, i soggetti che prestano servizi di certificazione di Firma Elettronica qualificata.

LE SANZIONI PREVISTE IN RELAZIONE Al REATI DI CUI AGLI ARTICOLI 491-8IS, 615-TER, 615-QUATER, 615-QUINQUIES, 617-QUATER, 617-QUINQUIES, 635-BIS, 635-TER, 635-QUATER, 635-QUINQUIES, 640-QUINQUIES

Con riferimento alle tipologie di Reati informatici espressamente previsti dall'art. 24- bis del D. Lgs. n. 231/01 e presi in considerazione nella presente Parte Speciale in quanto potenzialmente rilevanti per Promomedia, si riporta, di seguito, una tabella riepilogativa delle relative sanzioni previste a carico della Società qualora, per effetto della commissione dei reati indicati al precedente paragrafo 1 da parte dei Soggetti Apicali e/o dei Soggetti Sottoposti, derivi alla Società un interesse o un vantaggio.

Reato	Sanzione Pecuniaria	Sanzione Interdittiva
Accesso abusivo a un sistema informatico o telematico (art. 615- *ter* c.p.) intercettazione, impedimenta o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-quaterc.p.) installazione di apparecchiature atte a intercettare, impedire o interrompere comunicazioni informatiche o telematiche *(art.617-quinquies* c.p.) Danneggiamento di informazioni, dati e programmi informatici (art.635-bis c.p.) Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art.635-terc.p.) Danneggiamento di sistemi informatici o telematici (art. 635- quaterc.p.) Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635- *quinquies* c.p.)	Da 100 a 500 quote	art. 9, comma 2. lett. a), b), e) - interdizione dall'esercizio dell'attività; - sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito; - divieto di pubblicizzare bani o servizi
Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615- *quater* c.p.) Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (615- *quinquies* c.p.)	Fino a 300 quote	art. 9. comma 2. lett. b). e) sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito; divieto di pubblicizzare beni o servizi

Documenti informatici (art. 491-*bis* c.p.) Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. *640-quinquies* c.p.)	Fino a 400 quote	art. 9, comma 2, lett. c), d), e) - divieto di contrattare con la pubblica amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio; - esclusione da agevolazioni, finanziamenti, contributi o sussidi o eventuale revoca di quelli già concessi; - divieto di pubblicizzare beni o servizi

DESTINATARI DELLA PARTE SPECIALE

Destinatari della presente Parte Speciale sono tutti *i* Soggetti Apicali e i Soggetti Sottoposti che operano nelle "attività sensibili" o "a rischio-reato" di seguito identificate con riferimento alle fattispecie contemplate dall'art. 24-bis del D. Lgs. 231/01.

Tutti i destinatari della presente Parte Speciale sono tenuti ad adottare comportamenti conformi a quanto di seguito formulato, al fine di prevenire la commissione dei reati individuati nell'ambito della normativa di riferimento.

INDIVIDUAZIONE DELLE ATTIVITA SENSIBILI E DEI RUOLI AZIENDALI COINVOLTI

A seguito dell'attività di mappatura dei rischi, sono state individuate, nell'ambito della struttura organizzativa di Brain-it , le attività considerate "sensibili" rispetto alle fattispecie di reato indicate, ovvero quelle attività all'espletamento delle quali è potenzialmente connesso ii rischio di commissione dei reati in esame.

Nell'ambito dei reati ritenuti astrattamente ipotizzabili, sono state individuate le attività "sensibili" e i Ruoli/Funzioni coinvolti, come di seguito riportato.

In particolare, con riferimento ai reati di;

- ***Documenti informatici (art. 491-bis c.p.)***
- **Accesso *abusivo ad un sistema informatico* o *telematico* *(art. 615-terc.p.)***
- ***Detenzione* e *diffusione abusiva di codici di accesso a sistemi informatici* o *telematici* *(art. 615-quaterc.p.)***
- ***Diffusione di apparecchiature, dispositivi* o *programmi informatici diretti* a *danneggiare* o *interrompere un sistema informatico* o *telematico (art. 615- quinquies c.p.)***
- ***intercettazione, impedimento* o *interruzione illecita di comunicazioni informatiche* o *telematiche (art. 617-quaterc.p.)***
- ***installazione di apparecchiature atte ad intercettare, impedire* o *interrompere comunicazioni informatiche* o *telematiche (art. 617-quinquies c.p.)***
- ***Danneggiamento di informazioni, dati* e *programmi informatici (art. 635-bisc.p.)***
- ***Danneggiamento di informazioni, dati* e *programmi informatici utilizzati dallo Stato* o *da altro ente pubblico* o *comunque di pubblica utilità (art. 635-terc.p.)***
- ***Danneggiamento di sistemi informatici* o *telematici (art. 635-quaterc.p.)***
- ***Danneggiamento di sistemi IT* o *telematici di pubblica utilità (art. 635- quinquies c.p.)***

le *Attività sensibili* individuate sono le seguenti:

- *Utilizzo di strumenti e di sistemi informatici aziendali* *Accesso a connessioni di rete*
- *Gestione degli strumenti e dei sistemi informatici aziendali*
- *Gestione e manutenzione delle reti dell'infrastruttura informatica aziendale* *Accesso alle apparecchiature informatiche* o *telematiche aziendali.*
- *Ruoli e Funzioni coinvolti:*

    - Tutte le funzioni aziendali.

PRINCIPI E REGOLE DI COMPORTAMENTO

Tutte le attività sensibili devono essere svolte seguendo le leggi vigenti, i valori, le politiche e le procedure di Brain-it nonché le regole contenute nel presente Modello.

In generale, ii sistema di organizzazione, gestione e controllo della Società deve rispettare i principi di attribuzione di responsabilità e di rappresentanza, di separazione di ruoli e compiti e di lealtà, correttezza, trasparenza e tracciabilità degli atti.

Nello svolgimento delle attività sopra descritte e, in generale, delle proprie funzioni, gli Amministratori, gli Organi Sociali, i dipendenti, i procuratori, nonché i collaboratori e tutte le altre controparti contrattuali, devono conoscere e rispettare:

- la normativa italiana e straniera applicabile alle attività svolte;
- il Codice Etico Aziendale;
- il presente Modello;
- le procedure e le linee guida della Società, nonché tutta la documentazione attinente ii sistema di organizzazione, gestione e controllo della Società.

ATTIVITA' E PROCEDURE GENERALI DI PREVENZIONE

Brain-it ha provveduto ad adottare ii proprio "Codice Etico" al fine di promuovere ed assicurare l'osservanza di massimi standard di integrità individuale ed aziendale e la responsabilizzazione nello svolgimento delle attività, disciplinando tra l'altro:

- la limitazione dell'utilizzo dei sistemi informatici o telematici ai soli fini lavorativi;

- l'accesso alle informazioni aziendali solo previa autorizzazione da un livello gerarchico adeguato;

- l'accesso alle informazioni aziendali solo mediante gli strumenti concessi e autorizzati dalla Società;

- la riservatezza delle informazioni aziendali;

- l'elaborazione dei dati nel rispetto delle modalità previste dalle procedure aziendali;

- l'integrità dei dati elaborati;

- l'impossibilita di installare sui sistemi informatici/telematici aziendali software o hardware non autorizzati;

- l'impossibilita di introdurre in azienda dispositivi hardware/software non autorizzati.

I Soggetti coinvolti nella gestione delle attività rilevanti ex D. Lgs. 231/2001 sono tenuti, al fine di prevenire e impedire ii verificarsi di Reati informatici, al rispetto dei seguenti principi generali di condotta:

- astenersi dal porre in essere o partecipare alla realizzazione di condotte tali che, considerate individualmente o collettivamente, possano integrare le fattispecie di illecito riportate nella presente Parte Speciale;

- astenersi dal porre in essere ed adottare comportamenti che, sebbene non integrino, di per se, alcuna delle fattispecie dei reati indicati nella presente Parte Speciale, possano potenzialmente diventare idonei alla realizzazione dei reati medesimi.

Con riferimento alle attività ritenute rilevanti ai sensi del D. Lgs. 231/2001 ai fini dei Reati informatici è espressamente vietato:

- introdursi abusivamente in un sistema informatico o telematico protetto da misure di sicurezza contro la volontà del titolare del diritto di accesso;

- accedere al sistema informatico o telematico, o a parti di esso, ovvero a banche dati della Società, o a parti di esse, non possedendo le credenziali di accesso o mediante l'utilizzo di credenziali di altri colleghi abilitati;

- intercettare fraudolentemente e/o diffondere, mediante qualsiasi mezzo di informazione al pubblico, comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi;

- utilizzare dispositivi tecnici o strumenti software non autorizzati (ad esempio, virus, worm, troian, spyware, dialer, keylogger, rootkit) atti ad impedire o interrompere le comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi;

- distruggere, deteriorare, cancellare, alterare, sopprimere informazioni, dati o programmi informatici altrui o anche solo mettere in pericolo l'integrità e la disponibilità di informazioni, dati o programmi utilizzati dallo Stato o da altro ente pubblico o ad esso pertinenti o comunque di pubblica utilità;
- introdurre o trasmettere dati, informazioni o programmi al fine di distruggere, danneggiare, rendere in tutto o in parte inservibili, ostacolare ii funzionamento dei sistemi informatici o

telematici di pubblica utilità; detenere, procurarsi, riprodurre, o diffondere abusivamente codici di accesso o comunque mezzi idonei all'accesso di un sistema protetto da misure di sicurezza;

- procurare, riprodurre, diffondere, comunicare, mettere a disposizione di altri apparecchiature, dispositivi o programmi al fine di danneggiare illecitamente un sistema o i dati e i programmi ad esso pertinenti ovvero favorirne l'interruzione o l'alterazione del suo funzionamento;
- alterare, mediante l'utilizzo di firma elettronica o comunque in qualsiasi altro modo, e/o falsificare, documenti informatici;
- produrre e trasmettere documenti in formato elettronico contenenti dati falsi e/o alterati.

PROCEDURE SPECIFICHE

Gli Organi Sociali, gli Amministratori, i dipendenti ed i procuratori di Brain-it nonché i collaboratori e tutte le altre controparti contrattuali, dovranno tener conto, oltre a quanto precedentemente descritto relativamente alle fattispecie di reato ritenute rilevanti per la Società, delle previsioni di seguito indicate.

In dettaglio, i soggetti sopra citati devono rispettare le procedure e le regole aziendali che prevedono, tra l'altro:

- l'osservanza del "Regolamento di utilizzo degli strumenti elettronici - R.U.S.E", ii quale:
  - descrive ii concetto di "risorsa informatica", tale da includere anche eventuali soluzioni tecnologiche esistenti o future che i dipendenti della Società potranno utilizzare nell'ambito della propria attività lavorativa;
  - definisce i principi generali sull'assegnazione delle risorse informatiche e sulla formate attribuzione delle responsabilità circa il loro utilizzo (l'assegnazione delle responsabilità è univocamente identificata anche per le risorse informatiche condivise tra più utenti);
  - e vieta:
  - l'installazione autonoma di programmi provenienti dall'esterno, salvo previa autorizzazione esplicita del titolare del trattamento;
  - l'uso di programmi diversi da quelli scelti, distribuiti ed installati ufficialmente dal titolare del trattamento, e cioè brain-it;
  - la modifica delle caratteristiche impostate sul proprio PC, salvo previa autorizzazione esplicita del titolare del trattamento o del responsabile del trattamento del settore di riferimento;

- l'installazione sul proprio PC di qualsiasi dispositivo di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, etc.);
- l'assunzione di falsa identità nell'accedere ai sistemi o nell'inviare o dare seguito a comunicazioni informatiche o telematiche;
- l'effettuazione di intrusioni illecite in sistemi informatici, sia aziendali che esterni, mediante attività di hacking o cracking;
- la creazione e/o diffusione di virus informatici;
- la copiatura e/o la trasmissione di informazioni ottenute mediante accesso non autorizzato a un sistema informatico;

l'utilizzo delle risorse informatiche per canto o nell'interesse di soggetti terzi.

- la classificazione dei dati (e delle informazioni) aziendali secondo criteri ben definiti che tengono conto di integrità, riservatezza e disponibilità degli stessi;
- lo svolgimento di un'attività di formazione/informazione rivolta a tutti gli utenti aziendali che utilizzano le risorse informatiche o telematiche per le proprie attività lavorative;
- delle adeguate condizioni per la sicurezza fisica e ambientale del CED (Centro Elaborazione Dati) della Società che includono, tra l'altro, le modalità di registrazione degli accessi del personale autorizzato e del personale esterno;
- l'utilizzo di un *firewall*, configurato per la gestione e l'analisi degli accessi "da" e "verso" Internet, che gestisce ii punto di contatto tra internet e la rete aziendale, e la restrizione della navigazione in termini di siti visitabili mediante l'utilizzo di filtri specifici;
- delle review periodiche dei log, mediante l'ausilio di strumenti automatici, volte ad individuare eventuali attività non consentite o comportamenti anomali da parte degli utenti/amministratori di sistema, e la protezione dei log in scrittura per i soggetti che hanno operato sul Sistema, inclusi gli amministratori;
- l'utilizzo di un sistema di Intrusion Detection System al fine di monitorare ii traffico in ingresso nella rete;
- una comunicazione crittografata attraverso l'accesso da remoto, da parte del personale della Società e degli enti, mediante la Virtual Private Network (VPN); nello specifico gli enti sono abilitati ad accedere tramite VPN per verificare, in modalità di sola visualizzazione, le posizioni dei contribuenti e i relativi versamenti;
- l'ubicazione dei web server e-mail server della Società in una DMZ (delimitarized zone), al fine di permetterne l'accesso da internet (per ii regolare svolgimento dei servizi web e di pasta elettronica) senza compromettere la sicurezza della rete aziendale interna;

• il divieto di installazione e/o utilizzo su/da Personal Computer aziendale, di software provenienti dall'esterno, senza una specifica autorizzazione;

• il corretto utilizzo del collegamento ad Internet. In particolare:

- non è consentito navigare in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa stessa;

- non è consentito effettuare ii download di software gratuiti (freeware} e shareware prelevati da siti Internet, se non espressamente autorizzati dagli Amministratori di Sistema o dal Responsabile del Trattamento Dati di riferimento;

- non è consentito effettuare ogni genere di transazione finanziaria, ivi comprese le operazioni di remote banking, acquisti on-line e simili, salvo i casi direttamente autorizzati dalla Direzione Generale e con il rispetto delle normali procedure di acquisto;

- non è consentito registrarsi a siti i cui contenuti non siano legati all'attività lavorativa;

- non è consentito partecipare a forum non professionali, utilizzare chat line, bacheche elettroniche e registrazioni in guest books, anche utilizzando pseudonimi (o nicknames};

• l'utilizzo di uno strumento di *hardware/software inventory* volto ad individuare la presenza di software/hardware non autorizzati;

• l'utilizzo del sistema di posta elettronica aziendale per tutte le comunicazioni di carattere non pubblico;

• la tracciabilità dell'utilizzo dei sistemi mediante le seguenti tipologie di log:

o log del traffico di rete, al fine di acquisire informazioni relative a tutto ii traffico, da e verso l'esterno della rete;

o log di sistema, al fine di acquisire informazioni sui processi del sistema e sui servizi erogati, sull'evento accaduto (informazione, errore, etc.} e sulla sua entità, sull'accesso agli elaboratori e sull'utenza interessata;

• l'utilizzo con particolare cautela e diligenza dei supporti magnetici riutilizzabili (dischetti, cassette, cartucce, cd, dvd, pendrive, hard disk esterni, ecc.) contenenti dati inerenti alle attività aziendali;

• lo svolgimento periodico di un'attività di monitoraggio volta a verificare la presenza di eventuali software dannosi e l'esecuzione tempestiva di un'attività di ripristino del funzionamento dei sistemi;

• l'utilizzo di posta elettronica certificata (PEC) per le comunicazioni tra le aree aziendali coinvolte e gli enti dotati anch'essi di posta elettronica certificata; i certificati e le chiavi crittografiche sono gestiti mediante un'Autorità di Certificazione (CA} esterna;

- l'utilizzo di un software antivirus aggiornato quotidianamente in modo automatico;
- l'identificazione univoca di ciascun utente tramite apposita user-id e ii divieto di utilizzo di utenze generiche nello svolgimento delle attività ordinarie;
- l'accesso ai sistemi applicativi della Società mediante password crittografate di lunghezza minima di otto caratteri con almeno un carattere alfanumerico;
- la gestione e ii controllo degli accessi alle applicazioni informatiche, che prevedono:
    - l'identificazione degli utenti tramite apposita user-id in grado di assegnare in maniera univoca le responsabilità di ciascuna azione {l'utilizzo di gruppi di utenze è consentito solamente per specifiche ragioni, opportunamente documentate e approvate dal management);
    - l'utilizzo di un modulo standard per la creazione/modifica/cancellazione di una utenza;
    - l'approvazione del management per la creazione/modifica/cancellazione di una utenza;
    - la firma, da parte degli utenti, di una dichiarazione di comprensione delle condizioni di utilizzo dell'utenza;
    - ii mantenimento di un registro attraverso ii quale associare un dipendente a ciascun account create;
    - la disabilitazione tempestiva di tutte le utenze associate a persona che hanno cambiato ruolo o si sono dimesse dalla Società;
    - verifiche periodiche sulle utenze per rimuovere o disabilitare user-id ridondanti o non più necessarie;
    - l'adozione di un sistema di ticketing per la tracciatura di tutte le attività di gestione delle utenze e l'archiviazione di tutta la documentazione a supporto.
- la segregazione dei compiti per le attività che devono essere svolte da persone distinte nel rispetto della matrice SoD;
- ii blocco automatico delta sessione inattiva dopo 10 minuti;
- la gestione del *Change Managment/System Development Life Cycle* attraverso una procedura che prevede, tra l'altro:
    - l'individuazione dei ruoli coinvolti nelle varie fasi del processo;
    - i passaggi approvativi necessari per una corretta gestione del ciclo di vita del software {richiesta, analisi di requisiti, project plan, test plan, implementazione test di accettazione);
    - lo svolgimento di attività di testing per ogni modifica apportata a Sistema e la predisposizione di un apposite modulo *(User Acceptance Test)* contenente le sezioni per la descrizione del test di accettazione e l'approvazione per ii passaggio in produzione;
    - un modulo specifico per le richieste delle modifiche;

- l'adozione di un sistema di ticketing per la tracciatura di tutte le attività relative al processo di *change management* e l'archiviazione di tutta la documentazione a supporto;
- lo svolgimento delle attività di test in ambienti segregati da quello di produzione al fine di ridurre ii rischio di alterazione dei dati.

• ii monitoraggio della vulnerabilità del proprio parco applicative e l'aggiogamento dei Sistemi attraverso ii download di *patch* a seguito delle segnalazioni dei fornitori degli applicativi;

• l'adozione di misure di sicurezza per la gestione degli incidenti e la tracciabilità di tutte le problematiche riscontrate dagli utenti e comunicate alla Divisione Informatica della Società.

COMPITI DELL'ORGANISMO DI VIGILANZA

Fermi restando i compiti e le funzioni dell'OdV statuiti nella Parte Generale del presente Modello, ai fini della prevenzione dei Reati informatici, lo stesso è tenuto a:

• Verificare il contenuto da parte dei Soggetti Apicali e Sottoposti delle prescrizioni e dei comportamenti esposti ai precedenti paragrafi e nelle Procedure aziendali·

• monitorare l'efficacia delle procedure interne e delle regole di corporate governance *per la parte* dei Reati informatici;

• proporre e collaborare alla predisposizione delle istruzioni standardizzate relative ai comportamenti da seguire nell'ambito delle aree a rischio individuate nella presente Parte Speciale;

• esaminare eventuali segnalazioni provenienti dagli organi di controllo o da qualsiasi dipendente e a disporre degli accertamenti ritenuti necessari.

L'OdV svolge in piena autorità le proposte delle attività di monitoraggio e verifica, programmate e non, effettuando controlli specifici sulle attività connesse ai Reati informatici

A tal fine, all'OdV viene garantito libero accesso a tutta la documentazione aziendale rilevante.